

Passwortverwaltung

Da für jeden Dienst ein anderes Passwort verwendet werden sollte, ist ein Programm zur Verwaltung hilfreich: **KeePassX** ist *freie Software* und speichert zusätzliche Informationen und Passwörter verschlüsselt mit einem Masterpasswort.

Schritt 1: Software installieren

KeePassX kann unter <https://www.keepassx.org/> heruntergeladen werden.

Schritt 2: Sprache ändern

Sollte die Oberfläche von KeePassX englisch sein, kann dies wie folgt geändert werden:
Menüleiste Tools → **Preferences** (Einstellungen) → **Language** (Sprache)

Schritt 3: Neue Passwort-Datenbank erstellen

- Menüleiste **Datenbank** → **Neue Datenbank**
- Masterpasswort setzen und wiederholen. (Nachträgliche Änderung ist möglich.)

Die Passwort-Datenbank ist eine besonders wichtige Datei. Ihr Inhalt ist sehr sensitiv und sehr schwer rekonstruierbar. Deshalb ist es von entscheidender Bedeutung, dass das **Masterpasswort sicher und gut merkbar** ist – davon hängt die Sicherheit aller weiteren Passwörter ab. Ebenso wichtig ist, dass von der Datenbank **verlässliche und genügend häufige Datensicherungen** angefertigt werden.

Schritt 4: Passworteinträge erstellen

Nun können im linken Bereich Gruppen erstellt und geordnet werden. Jede Gruppe kann etliche Passworteinträge enthalten, die im rechten Bereich mit Rechtsklick erstellt werden.

Wichtig: Nachdem Änderungen vorgenommen wurden, müssen diese unbedingt gespeichert werden. (Sie gehen sonst beim Schließen des Programms verloren.)



Alternativ kann die Einstellung „automatisch speichern“ aktiviert werden:
Menüleiste Tools → **Allgemein** → **Automatisch nach jeder Änderung speichern**

Schritt 5: Passwörter verwenden

Ein in der Übersicht markiertes Passwort kann mittels Copy-Paste (Strg+C und Strg+V) für kurze Zeit in die Zwischenablage kopiert und anschließend eingefügt werden. So wird das Passwort zu keiner Zeit im Klartext auf dem Bildschirm sichtbar.

Schritt 6: Was man mit Passwörtern *nicht* machen sollte

- Passwörter niemals durchs Netz schicken. Einzige Ausnahme: Der Zweck, zu dem es erzeugt wurde (Login etc.). Ein Passwort, das z.B. durchs Netz geschickt wurde, um dessen „Sicherheit“ zu überprüfen, ist ein verbranntes Passwort.
- Browser-AddOns zur Passwortverwaltung/Überprüfung meiden.
- Ein Passwort, dessen Eingabe gefilmt wurde, ist ein verbranntes Passwort. Auch im Bus oder der Bahn. Auch im Restaurant, das eigentlich nur die Angestellten filmen will.

Alternative für die Kommandozeile

Auf der Kommandozeile kann das Programm **pass** verwendet werden, das Passwörter in GPG-verschlüsselten Dateien vorhält.